

REMARKS

Claims 130-133 are the claims currently pending in the Application.

Rejection of Claims 130-133 under 35 U.S.C. § 103

Claims 130-133 are rejected under 35 U.S.C. § 103 as being obvious from Muratani et al., U.S. Patent No. 6,061,451 and Ruppert et al., U.S. Patent No. 5,640,002 in view of Perlman, U.S. Patent No. 5,175,765. This rejection is traversed.

Among the problems recognized and solved by Applicant's claimed invention is that a public key for a digital signature for authenticating digital data, such as for example a digital image, be transmitted as part of the same data set as the digital data.¹ By way of example, according to an aspect of Applicant's claimed invention, a digital signature is inserted into a predetermined bits portion of the digital data, such as into a least significant bit plane of the digital data, and this digital signature is then used to authenticate the digital data using the public key.

For at least the following reasons, Applicant's claimed invention is neither anticipated by nor obvious from the cited references. By way of example, independent claims 130-133 require inserting received data comprising a digital signature including a public key into a predetermined bits portion of the digital data, the digital data comprising an image data content file, a video data content file or an audio data content file.

¹ The present discussion illustrates aspects of Applicant's claimed invention. Applicant does not represent that every embodiment of Applicant's claimed invention necessarily embodies or performs the solutions herein discussed or addresses the problems herein identified.

Muratani discloses decrypting data that is received in an encrypted form from a network (Muratani, Abstract); for example, encrypted data received via a settop unit is descrambled by a descramble circuit of a security module that is connected to the settop unit (Muratani, Abstract; Fig. 2).

The Examiner acknowledges that Muratani does not disclose or suggest a digital signature inserted into the digital data, nor inserting a public key for the digital signature into a predetermined bits portion of the digital data (or into the digital image, per claim 133), as *inter alia*, required by independent claims 130-133. However, the Examiner also cites Ruppert.

Ruppert discloses a portable radio frequency bar code ID tag reader of the type used for example, at a supermarket checkout to authenticate articles by accessing a factory computer using the serial number of the article scanned from a radio frequency ID tag on the article. (Ruppert, Abstract.) Ruppert discloses that a computer sends its public key to a factory host computer (Ruppert, Figure 41, Reference Numeral 749); and that the factory computer uses its secret key to authenticate a serial number list, generates an authentication message, generates authentication signature of the message, and encrypts the authentication signature and authentication signature message using the public key (Ruppert, Figure 41, Reference Numerals 753-759).

The Examiner acknowledges that Muratani and Ruppert do not disclose or suggest inserting the received data comprising a public key for a digital signature into a predetermined bits portion of the digital data, as *inter alia* required by independent claims 130-133 (Office Action, page 4). However, the Examiner

cites Perlman, Fig. 2 and associated text and alleges that Perlman discloses that the data received includes a digital signature and public key.

Perlman discloses a public-key encryption system to authenticate data packets transmitted between nodes of a network (Perlman, Abstract), such that a public-key field 40 of the data packet 30 contains the public key associated with the originating node (Perlman, Fig. 2; col. 6, lines 25-34), used to authenticate the data packet against malicious failures.

Perlman does not disclose or suggest inserting a public key into digital data, the digital data comprising an image data content file, a video data content file and an audio data content file, as *inter alia* required. As discussed, Perlman is concerned with authenticating data packets, but is silent with respect to authenticating an image data content file, a video data content file or an audio data content file.

Therefore, since Perlman does not disclose or suggest this feature, Perlman is incapable of disclosing or suggesting inserting received data comprising a public key into the predetermined bits portion of the digital data, the digital data comprising an image data content file, a video data content file or an audio data content file as *inter alia* required by independent claims 130-132. Moreover, Perlman does not disclose or suggest inserting the received data comprising a public key for a digital signature into a predetermined bits portion of the digital image, as *inter alia* required by independent claim 133.

In fact, the cited references belong to the conventional art recognized by Applicant's disclosure, because the cited references do not disclose or suggest a significant insight provided by Applicant's invention: as discussed, according to an

aspect of Applicant's claimed invention, a digital signature is inserted into a predetermined bits portion of an image data content file, a video data content file or an audio data content file (that is, the predetermined bits portion of the digital data), for example, inserted into a least significant bit plane of the content file, and this digital signature is then used to authenticate the file using the public key.

In short, the cited references belong to the conventional art for at least the reason that they do not disclose or suggest the solution of inserting a public key into a predetermined bits portion of an image data content file, a video data content file or an audio data content file. Therefore, the cited references, even taken in combination, do not even remotely disclose Applicant's invention as claimed in independent claims 130-133. Accordingly, this rejection should now be withdrawn.

For at least the reasons set forth in the foregoing discussion, Applicant believes that the Application is now allowable and respectfully requests that the Examiner reconsider the rejections and allow the Application. Should the Examiner have any questions regarding this Amendment, or regarding the Application generally, the Examiner is invited to telephone the undersigned attorney.

Respectfully submitted,



Paul J. Esatto, Jr.
Registration No. 30,749

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza
Suite 300
Garden City, New York 11530
(516) 742-4343
PJE:ar